



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/911,042	07/23/2001	Takumi Okaue	SONYJP 3.0-190	3744
530 7590 04/11/2008 LERNER, DAVID, LITTENBERG, KRUMHOLZ & MENTLIK 600 SOUTH AVENUE WEST WESTFIELD, NJ 07090				
EXAMINER				
POPHAM, JEFFREY D				
ART UNIT		PAPER NUMBER		
2137				
MAIL DATE		DELIVERY MODE		
04/11/2008		PAPER		

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

09/911,042

Applicant(s)

OKAUE, TAKUMI

Examiner

JEFFREY D. POPHAM

Art Unit

2137

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 1-24.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-24 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-24 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 23 July 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some * c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
- Paper No./Mail Date: _____

- 4) ☐ Interview Summary (PTO-413)
- Paper No(s)/Mail Date: _____
- 5) ☐ Notice of Informal Patent Application
- 6) ☐ Other: _____

Remarks

Claims 1-24 are pending.

Response to Arguments

1. Applicant's arguments filed 1/14/2008 have been fully considered but they are not persuasive.

Applicant argues that neither Ueda nor Proudler disclose executing mutual authentication between a first structure and a virtual storage device when a memory of an external storage device does not store a ciphering key used when carrying out such mutual authentication. As previously pointed out, the specification of the current application does not refer to any "virtual storage" and therefore, this has been taken as a synonym for "virtual memory". Although the specification never defines a "virtual memory device", page 61, paragraph 272 of the specification refers to a virtual memory card as "a virtual memory card (the "Memory Stick", a product and registered trade name of Sony Corporation)". Therefore, this "virtual storage device" referred to in the claims can be a physical device. Therefore, a smart card (such as in Proudler) or SD memory card can be seen as a virtual storage device, much in the same way as a Memory Stick can be seen as a virtual storage device. As set forth in the 112 rejections below, the newly added negative limitation is not found within the application as originally filed, and further arguments regarding the references are discussed therewith.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

2. Claims 1-24 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim 1 was amended to include the negative limitation that "the memory does not store a ciphering key used when carrying out such mutual authentication". The other independent claims were amended in line with this. The Examiner cannot find basis for this limitation in the application as originally filed. The specification does refer to storing authentication keys in the memory of the storage device (pages 28-29) and storing authentication keys in a virtual memory card, such as a Memory Stick (pages 61-62), however, there is no disclosure regarding not storing a ciphering key used when carrying out mutual authentication in the memory of the external storage device. As seen in the specification, page 62, paragraph 275, the virtual memory card is loaded with an authentication key described in reference to figure 16. Figure 16 and the related portion of the specification relate to data stored in the memory of the storage device, however, and loading the virtual memory card with such data appears to comprise loading this data from the memory of the storage device itself. Therefore, the loading of the key from Ueda's external storage device into the virtual storage device and

performing mutual authentication using such is in line with what is disclosed in the instant application. In any case, even if the authentication key was not to be loaded from the external storage device, there is still not disclosure regarding not storing a ciphering key used when carrying out mutual authentication.

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1-24 are also rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

It is unclear how this ciphering key, such as provided in amended claim 1, that is not stored in the memory of the external device, is used for mutual authentication. The claims never use this ciphering key for any mutual authentication, only state that it is "used when carrying out such mutual authentication". Claims dependent upon claim 1 refer to other keys, that are distinct from such a ciphering key, being used for mutual authentication, and it is unclear how this ciphering key would be used when carrying out such mutual authentication. Some of the indefiniteness and ambiguity that this new limitation brings to light are now set forth.

It is noted that there is distinction between certain keys in the claims. In amended claim 1, for example, the memory does not store a ciphering key used when carrying out mutual authentication. Claim 3, on the other hand, refers to keys used in authentication as "a further key is provided for authenticating distribution of an enabling

key block", which is referred to later in claim 3 as "said enabling key block distribution authenticating key", and another authentication key referred to as "another authenticating key". One will note that neither of these keys used in authentication are "ciphering keys".

It is additionally noted that none of the claims refer to this ciphering key that is not stored in the memory as being used in any authentication or other processing whatsoever, it is simply an independent key used for nothing, and not being stored in the memory (the "used when carrying out such mutual authentication" portion of this limitation is discussed below). The claims clearly distinguish this key from all other keys, in that this key that is not stored and is used for nothing. In other words, this ciphering key is never stored, used, or cared about within the claims; it is simply not there and appears to have no purpose in ever being in any part of the system. From the above discussion, one can see that this limitation could mean nothing within the claims, merely not storing a key that is never used is insignificant.

However, one could also view the limitation as referring to a key that is still used in mutual authentication, such a key not being stored in memory of the external storage device, despite the fact that the key is never used in any portion of the claims for any positive authentication processing, merely described as "used when carrying out such mutual authentication". This could, therefore, be any key that is used during mutual authentication, for example, a key stored in the apparatus. The time variable key of Ueda fits this description, in that it is used during mutual authentication, but not stored in memory of the external storage device. Additionally, any keys used in mutual

authentication within Proudler would fit this description as well, since none are stored on the external storage device of the combination.

This also brings up the question about what is being mutually authenticated within the claims. If no data of the external storage device is being used in the mutual authentication, the external storage device is not one of the parties being mutually authenticated. Two portions of the apparatus may be mutually authenticating, however, as is the case where a smart card and another portion of the apparatus authenticate each other to ensure that the apparatus's integrity is verified and can be trusted. Perhaps a piece of data could be construed as one side of the mutual authentication with the apparatus as the other side, such that, if the apparatus can confirm that a certain piece of data (e.g. a license) is meant for the apparatus, mutual authentication has completed successfully (this is not normal mutual authentication, but could be construed as the apparatus authenticating that the data is proper, since the data is meant for the apparatus, and since the data is meant for the apparatus, the proper apparatus accessing the data provides for authentication of the apparatus to the data). It could also be data stored on the external storage device, that may not be a key, such as a license, that allows access to the data stored on the external storage device when an apparatus can authenticate that it is proper, authentic, and/or authorized to use such license and data. A few different interpretations regarding this ambiguity have been found in the references cited in the conclusion section of this office action.

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1, 8, 12, 13, 20, and 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ueda (U.S. Patent 6,289,102) in view of Proudler (U.S. Patent 7,236,455).

Regarding Claim 1,

Ueda discloses a data processing apparatus for receiving data from or delivering data to a storage device, the storage device being external to the data processing apparatus and including a memory, the data received from the external storage device being reproduced from the memory and the data delivered to the external storage device being recorded in the memory, the receiving or delivering ordinarily being carried out on condition that mutual authentication between the data processing apparatus and the storage device is successful, the data processing apparatus comprising:

A virtual storage device and a first structure each operable to alternatively execute mutual authentication between the first structure and the virtual storage device when the external storage device does not include any structure operable to execute the mutual authentication and is not operable to enable such mutual authentication and the memory does

not store a ciphering key used when carrying out such mutual authentication, the mutual authentication thereby being carried out solely within the data processing apparatus (Figures 14-16; Column 23, lines 26-61; and Column 37, lines 5-40); and

A second structure operable to receive the data from the external storage device or to deliver data to the external storage device when the mutual authentication between the first structure and the virtual storage device is successful (Figures 14-16; Column 23, line 49 to Column 24, line 17; and Column 25, lines 1-16).

Proudler also discloses a virtual storage device and a structure operable to alternatively execute mutual authentication between the structure and the virtual storage device in order to gain access to the apparatus, and the components thereof and connected to such apparatus (Column 9, lines 4-11; and Column 12, line 47 to Column 13, line 49). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the trusted device mutual authentication processing of Proudler into the recording and reproducing system of Ueda in order to increase the level of trust and security in the entire apparatus and/or to ensure that both a proper smart card and trusted platform authenticate each other before use thereof is allowed, while maintaining such trust and security while the platform is in use.

Regarding Claim 8,

Claim 8 is a method claim that is broader than apparatus claim 1 and is rejected for the same reasons.

Regarding Claim 12,

Claim 12 is a computer readable medium claim that is broader than apparatus claim 1 and is rejected for the same reasons.

Regarding Claim 13,

Claim 13 is an apparatus claim that is broader than apparatus claim 1 and is rejected for the same reasons.

Regarding Claim 20,

Claim 20 is a method claim that is broader than apparatus claim 1 and is rejected for the same reasons.

Regarding Claim 24,

Claim 24 is a computer readable medium claim that is broader than apparatus claim 1 and is rejected for the same reasons.

5. Claims 2, 9, 14, and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ueda in view of Proudler, further in view of Ansell (U.S. Patent 6,367,019).

Regarding Claim 2,

Ueda as modified by Proudler does not disclose initially checking whether the external storage device includes a structure operable to execute the mutual authentication.

Ansell, however, discloses initially checking whether the external storage device includes a structure operable to execute the mutual authentication (Column 12, lines 30-41). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the copy security system of Ansell into the recording and reproducing system of Ueda in order to allow copyrightable content of digital storage media to be protected against unauthorized copying, whether the storage media is functional or non-functional.

Regarding Claim 9,

Claim 9 is a method claim that is broader than apparatus claim 2 and is rejected for the same reasons.

Regarding Claim 14,

Claim 14 is an apparatus claim that is broader than apparatus claim 2 and is rejected for the same reasons.

Regarding Claim 21,

Claim 21 is a method claim that is broader than apparatus claim 2 and is rejected for the same reasons.

6. Claims 3, 5-7, 10, 15, 17-19, and 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ueda in view of Proudler, further in view of Dondeti (U.S. Patent 6,240,188).

Regarding Claim 3,

Ueda as modified by Proudler discloses the apparatus of claim 1, in addition, Ueda discloses that the first structure and the virtual storage device execute the mutual authentication between the first structure and the virtual storage device by applying a distributed key and another authenticating key previously stored in the virtual storage device (Figures 14-16; Column 23, line 26 to Column 24, line 17; and Column 37, line 5 to Column 38, line 51);

But does not disclose a further key is provided for authenticating distribution of an enabling key block, the further key having been previously enciphered by the enabling key block, the enabling key block containing enciphering data for enciphering renewal keys which are located on various paths of a hierarchical key tree structure, the hierarchical tree structure having a plurality of keys associated with various roots of the tree structure, nodes of the tree structure, and leaves of the tree structure, whereby a given one of the plurality of paths of the key tree structure extends from a specific one of the roots to a particular one of the leaves of the key tree structure, the leaves of the tree structure being respectively associated with a plurality of data processing apparatuses, the enciphering data including upper-rank keys in the tree hierarchy which are enciphered by lower-rank keys.

Dondeti, however, discloses that a further key is provided for authenticating distribution of an enabling key block, the further key having

been previously enciphered by the enabling key block, the enabling key block containing enciphering data for enciphering renewal keys which are located on various paths of a hierarchical key tree structure, the hierarchical tree structure having a plurality of keys associated with various roots of the tree structure, nodes of the tree structure, and leaves of the tree structure, whereby a given one of the plurality of paths of the key tree structure extends from a specific one of the roots to a particular one of the leaves of the key tree structure, the leaves of the tree structure being respectively associated with a plurality of data processing apparatuses, the enciphering data including upper-rank keys in the tree hierarchy which are enciphered by lower-rank keys (Column 3, line 48 to Column 4, line 21). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the hierarchical key tree structure of Dondeti into the recording and reproducing system of Ueda in order to make the system scalable to allow for the additional and modification of many processing apparatuses.

Regarding Claim 10,

Claim 10 is a method claim that is broader than apparatus claim 3 and is rejected for the same reasons.

Regarding Claim 15,

Claim 15 is an apparatus claim that is broader than apparatus claim 3 and is rejected for the same reasons.

Regarding Claim 22,

Claim 22 is a method claim that is broader than apparatus claim 3 and is rejected for the same reasons.

Regarding Claim 5,

Ueda as modified by Proudler and Dondeti discloses the apparatus of claim 3, in addition, Dondeti discloses means for subjecting the enabling key block distribution authenticating key to a version controlling process by executing a process for renewing individual versions (Column 1, lines 30-46; and Column 3, line 48 to Column 4, line 21).

Regarding Claim 17,

Claim 17 is an apparatus claim that is broader than apparatus claim 5 and is rejected for the same reasons.

Regarding Claim 6,

Ueda as modified by Proudler does not disclose that a key tree structure is provided comprising a plurality of keys associated with various roots of the tree structure, nodes of the tree structure, and leaves of the tree structure, and having a plurality of paths whereby a given one of the paths extends from a specific one of the roots to a particular one of the leaves of the key tree structure, a plurality of data processing apparatuses being respectively associated with the leaves of the tree, and the data processing apparatus further comprises: means for enciphering leaf-keys associated with the leaves using a storage key that is proper to an

individual one of the data processing apparatuses and then storing the enciphered leaf-key in a memory means within a corresponding data processing apparatus.

Dondeti, however, discloses that a key tree structure is provided comprising a plurality of keys associated with various roots of the tree structure, nodes of the tree structure, and leaves of the tree structure, and having a plurality of paths whereby a given one of the paths extends from a specific one of the roots to a particular one of the leaves of the key tree structure, a plurality of data processing apparatuses being respectively associated with the leaves of the tree (Column 3, line 48 to Column 4, line 21), and the data processing apparatus further comprises: means for enciphering leaf-keys associated with the leaves using a storage key that is proper to an individual one of the data processing apparatuses and then storing the enciphered leaf-key in a memory means within a corresponding data processing apparatus (Column 3, line 48 to Column 4, line 21). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the hierarchical key tree structure of Dondeti into the recording and reproducing system of Ueda in order to make the system scalable to allow for the additional and modification of many processing apparatuses.

Regarding Claim 18,

Claim 18 is an apparatus claim that is broader than apparatus claim 6 and is rejected for the same reasons.

Regarding Claim 7,

Ueda as modified by Proudler does not disclose that a key tree structure is provided comprising a plurality of keys respectively associated with various roots of the tree structure, nodes of the tree structure, and leaves of the tree structure, and having a plurality of paths that extend from the roots to the leaves of the key tree structure, a plurality of data processing apparatuses respectively corresponding to the leaves of the tree and to leaf-keys that further correspond with the leaves; and a device key block is stored in a memory within the processing apparatus, the key block being an assemblage of ciphered keys comprising mutually different individually enciphered node keys of plural steps extending from the leaves of the tree structure up to upper-rank keys of the tree structure.

Dondeti, however, discloses that a key tree structure is provided comprising a plurality of keys respectively associated with various roots of the tree structure, nodes of the tree structure, and leaves of the tree structure, and having a plurality of paths that extend from the roots to the leaves of the key tree structure, a plurality of data processing apparatuses respectively corresponding to the leaves of the tree and to leaf-keys that further correspond with the leaves (Column 3, line 48 to Column 4, line 21); and a device key block is stored in a memory within the processing

apparatus, the key block being an assemblage of ciphered keys comprising mutually different individually enciphered node keys of plural steps extending from the leaves of the tree structure up to upper-rank keys of the tree structure (Column 3, line 48 to Column 4, line 21). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the hierarchical key tree structure of Dondeti into the recording and reproducing system of Ueda in order to make the system scalable to allow for the additional and modification of many processing apparatuses.

Regarding Claim 19,

Claim 19 is an apparatus claim that is broader than apparatus claim 7 and is rejected for the same reasons.

7. Claims 4, 11, 16, and 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ueda in view of Proudler and Dondeti, further in view of Harada (U.S. Patent 6,850,914).

Regarding Claim 4,

Ueda as modified by Proudler and Dondeti discloses the apparatus of claim 3, in addition, Dondeti discloses that only a proper data processing apparatus is enabled to decode the enabling key block, whereas an improper apparatus is unable to decode the enabling key block (Column 3, line 48 to Column 4, line 21); but does not disclose the

use of licensing the determine which data processing apparatuses are proper and which are not, or revoking improper data processing apparatuses.

Harada, however, discloses the use of licenses to determine which data processing apparatuses are proper and which are not and revoking an improper data processing apparatus (Column 5, lines 15-67). It would have been obvious to one of ordinary skill in the art at the time of applicant's invention to incorporate the licensing and revocation system of Harada into the recording and reproducing system of Ueda as modified by Dondeti in order to provide for dynamic revocation of data processing apparatuses, such that revocation lists can be updated in a timely and efficient manner, thus allowing all proper apparatuses to know which other apparatuses are proper and which are revoked.

Regarding Claim 11,

Claim 11 is a system claim that is broader than apparatus claim 4 and is rejected for the same reasons.

Regarding Claim 16,

Claim 16 is an apparatus claim that is broader than apparatus claim 4 and is rejected for the same reasons.

Regarding Claim 23,

Claim 23 is a system claim that is broader than apparatus claim 4 and is rejected for the same reasons.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Story (U.S. Patent Application Publication 2002/0046181)

Matyas (U.S. Patent 4,757,534)

Lotspiech (U.S. Patent 6,609,116)

Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEFFREY D. POPHAM whose telephone number is (571)272-7215. The examiner can normally be reached on M-F 9:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571)272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Jeffrey D Popham
Examiner
Art Unit 2137

/Jeffrey D Popham/
Examiner, Art Unit 2137

/Emmanuel L. Moise/
Supervisory Patent Examiner, Art Unit 2137